*УДК 351.746(100)*
DOI 10.32755/sjlaw.2025.03.019

**Крушеніцький В. С.,**
аспірант кафедри права та правоохоронної діяльності,
Центральноукраїнський державний університет
імені Володимира Винниченка,
м. Кропивницький, Україна
ORCID: 0000-0001-9194-7897

# ЗАРУБІЖНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ У ПУБЛІЧНО-ІНФОРМАЦІЙНІЙ СФЕРІ

*У статті здійснено комплексний аналіз міжнародних моделей забезпечення інформаційної безпеки в умовах глобалізації, цифрової трансформації та зростання гібридних загроз. На основі проведеного аналізу запропоновано шляхи вдосконалення системи інформаційної безпеки України, зокрема шляхом створення єдиного національного координаційного органу, гармонізацію законодавства з європейськими нормами, впровадження цифрової освіти, розширення міжнародної співпраці та забезпечення громадського контролю.*

***Ключові слова:*** *інформаційна безпека, кібербезпека, національна безпека, стратегія безпеки, цифрова трансформація, кіберінфраструктура, критична інфраструктура, кіберзахист, дезінформація, цифрова грамотність, міжнародна співпраця, правове регулювання, стратегічні комунікації.*

**Постановка проблеми.** У сучасному глобалізованому світі питання забезпечення національної безпеки у публічно-інформаційній сфері набуває особливої актуальності, адже інформаційний простір став ареною геополітичного протистояння, кіберзагроз і дезінформаційних кампаній. В умовах гібридних війн, втручання у внутрішні справи держав через інформаційні ресурси та загрози стратегічним комунікаціям, зростає потреба у вивченні зарубіжного досвіду протидії таким викликам. Багато країн уже розробили ефективні моделі регулювання, захисту кіберпростору, а також взаємодії між державними інституціями та суспільством у сфері інформаційної безпеки. Однак для України досі актуальним залишається питання адаптації кращих практик з урахуванням національних особливостей, що зумовлює потребу у ґрунтовному аналізі та узагальненні міжнародного досвіду у цій галузі.

**Аналіз останніх досліджень та публікацій.** Проблематика інформаційної безпеки та зарубіжного досвіду її забезпечення знайшла відображення у працях таких авторів, як: О. Бандурки, І. Боднар, Н. Грабар, Д. Дубова, Б. Леонова, В. Пилипчука, В. Петрова, М. Погорецького, В. Пугачова, М. Стрельбицького та ін.

**Мета статті** дослідити зарубіжні моделі забезпечення національної безпеки в публічно-інформаційній сфері, проаналізувати їхні інституційні, правові та технологічні аспекти, а також визначити можливості імплементації ефективних практик в українське законодавство і державну політику.

**Виклад основного матеріалу.** У сучасних умовах глобалізації, динамічного розвитку цифрових технологій та поширення гібридних загроз питання інформаційної безпеки постає як пріоритетне у системі національної безпеки кожної держави. Вивчення зарубіжного досвіду у цій сфері дозволяє окреслити ефективні моделі, що забезпечують стійкість інформаційного простору, та визначити вектори подальшого розвитку для країн, які прагнуть адаптувати ці практики, зокрема для України.

Однією з найрозвиненіших є модель Сполучених Штатів Америки, яка ґрунтується на інтеграції зусиль державних, військових та приватних структур у межах уніфікованої стратегії. Основними інституціями є Департамент внутрішньої безпеки (DHS), Національне агентство з безпеки (NSA) та Командування кіберпростору США (USCYBERCOM). Ці органи забезпечують координацію заходів щодо захисту критичної інфраструктури, інформаційних систем, а також протидію зовнішньому втручанню в демократичні процеси. У США існує розвинена система стратегічних комунікацій, що забезпечує оперативне реагування на спроби дезінформації. Законодавчо закріплено принципи кібергігієни, відповідальність цифрових платформ, а також налагоджено ефективну міжвідомчу взаємодію. Особливої уваги заслуговує масштабне фінансування досліджень у сфері штучного інтелекту, який застосовується для автоматизованого аналізу інформаційних потоків, виявлення аномалій і загроз у реальному часі.

Європейський Союз реалізує модель гармонізації підходів до інформаційної безпеки на рівні держав-членів. У 2001 році Європейська Комісія представила перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід» [1; 2]. Цей документ, презентований Європейською Комісією у 2001 році, став важливим кроком у формуванні загальноєвропейської стратегії забезпечення інформаційної безпеки. У ньому було визначено основні проблеми, що виникають у зв'язку з інформаційною безпекою, та запропоновано політичний підхід до їх розв'язання на рівні ЄС. Документ заклав фундамент для подальших ініціатив і розробок у цій сфері, ставши своєрідним орієнтиром для держав-членів ЄС у побудові їхніх національних стратегій. Основні ідеї та підходи, викладені в документі, стали базисом для розроблення подальших політик та нормативних актів у сфері мережевої та інформаційної безпеки в ЄС. Вони вплинули на створення такої ініціативи, як Директива про безпеку мережевих та інформаційних систем (NIS Directive), яка була прийнята у 2016 році, і яка зобов'язує держави-члени ЄС впроваджувати мінімальні стандарти кібербезпеки на національному рівні [1; 3]. У межах ЄС активно впроваджуються програми підвищення цифрової грамотності громадян, а також інтегруються модулі інформаційної безпеки до системи загальної та вищої освіти. Особливе значення надається прозорості державної політики, доступу громадян до інформації і громадському контролю.

Франція трактує інформаційну безпеку як невід'ємну складову стратегії національної безпеки. Основи цієї політики викладені у так званих Білих книгах оборони та національної безпеки. З 1972 року в цих документах послідовно розвивається концепція інтегрованої безпеки, що охоплює як оборонний, так і цивільний виміри. Після завершення холодної війни акценти змістилися на зовнішні військові операції, професіоналізацію армії та інформаційну безпеку. У Білій книзі 2008 року вперше докладно проаналізовано загрози, що походять від кіберзлочинності, масштабних атак на інформаційні системи, а також використання ЗМІ та інтернету як інструментів

маніпуляції, шпіонажу та стратегічного впливу. У Франції діє розгалужена інституційна система: ANSSI координує заходи з кіберзахисту, DISIC відповідає за державні комунікації, а спеціалізовані служби займаються контрпропагандою та інформаційною протидією [4, с. 189].

Досвід Естонії, однієї з країн Балтії, відзначається впровадженням моделі «електронної держави». В основі її – потужна кіберінфраструктура, повна цифровізація адміністративних процесів, висока якість цифрової освіти та ефективне публічно-приватне партнерство. Естонія досягла одного з найвищих рівнів цифрової ідентифікації громадян, що забезпечує не лише безпеку даних, а й довіру населення до державних електронних сервісів.

Щодо досвіду Польщі, то основне завдання у справі забезпечення кібернетичної безпеки покладено на Агентство внутрішньої безпеки (ABW). Ним 2013 року було здійснено розробку Стратегії кібербезпеки Польщі, крім того, Агентство виступило з ініціативою створити Центр криптології при Міністерстві національної оборони, що має захищати інформацію, здійснювати кібероборону й вести наступальні кібероперації [1]. ABW також створило урядову команду реагування на комп'ютерні інциденти (CERT), головним завданням якої є «забезпечення і розвиток можливостей органів державного управління щодо захисту від кіберзагроз, зокрема від атак на інфраструктуру, що складається з IT-систем та комп'ютерних мереж, порушення роботи або руйнація яких може значною мірою загрожувати життю і здоров'ю людей, національним багатствам та навколишньому середовищу або призвести до значних фінансових збитків і збоїв у функціонуванні органів державної влади» [1; 5, с. 79]. Оскільки зросли інформаційні гібридні загрози, що, приміром, мають ознаки пропаганди, дезінформації або психологічного залякування, які здійснюють інші держави й недержавні виконавці (терористичні та інші організації), Бюро національної безпеки Польщі (BBN) 2015 року взялося за розроблення національної Доктрини інформаційної безпеки. Щоб чинити опір негативним тенденціям, рекомендовано «розпізнавати

інформаційне середовище, в тому числі визначати дружні, нейтральні і ворожі суб'єкти» [1]. Доктриною польської інформаційної безпеки вважають виконавчий документ, яким володіє Стратегія національної безпеки.

У Німеччині правовою основою для формування політики кібербезпеки є Закон про посилення безпеки IT-систем від 2015 року. Цей документ закріплює визначення критичної інфраструктури (енергетика, транспорт, охорона здоров'я тощо) та надає Федеральному відомству з безпеки у сфері IT (BSI) провідну роль у захисті державних і приватних цифрових систем. Командування стратегічної розвідки Бундесверу здійснює управління сучасними супутниковими системами SAR-Lupe та SATCOMBw, які забезпечують високоточну розвідку і безпечний зв'язок. Запровадження споживчого маркування IT-безпеки для комерційних продуктів є свідченням комплексного підходу до безпеки цифрового простору [4, с. 189].

Ізраїль реалізує концепцію активного кіберзахисту, що містить не лише оборону, а й превентивні дії. Тісна інтеграція армії, спецслужб, наукових інститутів і стартапів забезпечує розроблення інноваційних рішень, які дозволяють ефективно захищати критичну інфраструктуру.

Сучасна інфраструктура кібербезпеки в Ізраїлі охоплює приблизно 450 компаній, включно з відомими фірмами, такими як «Check Point», а також численні стартапи та венчурні фонди, зокрема «Jerusalem Venture Partners (JVP) Cyber Labs», що активно інвестують у цю галузь. Крім того, значну роль відіграють науково-дослідні проєкти, які сприяють співпраці між високотехнологічними компаніями та дослідницькими центрами [6, с. 79].

У 2017 році інвестиції у сферу кіберзахисту в Ізраїлі становили 10,8 мільйона доларів, що на 26 % більше порівняно з 2016 роком. На сьогодні Ізраїль є другим за обсягом експортером програмного забезпечення у світі після США. Таким чином, Ізраїль перетворюється з постачальника стартапів на міжнародний центр високих технологій, і, перш за все, стає одним із провідних світових лідерів у галузі кібербезпеки [6, с. 79; 7].

У червні 2018 року Ізраїльський національний кібердиректорат (INCD) оприлюднив проєкт закону про кібербезпеку для обговорення громадськістю. Цей проєкт закону спрямований на регулювання діяльності INCD відповідно до рішень уряду та є завершальною стадією створення національної кібербезпекової структури. Документ містить три основні розділи: 1) організаційний розділ визначає структуру та організаційні аспекти INCD; 2) оперативний розділ описує повноваження щодо виявлення та реагування на кібератаки; 3) регуляторний розділ встановлює національні та секторальні регуляції, спрямовані на підвищення стійкості різних секторів і визначає роль INCD як національного регулятора у сфері кібербезпеки [6, с. 79; 7].

Тобто ізраїльська модель кібербезпеки є яскравим прикладом ефективного синтезу державної політики, технологічного розвитку та стратегічного мислення. Вона базується на активному, а не реактивному підході до кіберзагроз, що дозволяє Ізраїлю не лише швидко реагувати на атаки, а й випереджати потенційні загрози.

Так, протягом 2019–2020 років INCD провів понад 30 зустрічей з різними зацікавленими сторонами, установами та урядовими міністерствами для обговорення коментарів щодо цього проєкту закону. На основі цих обговорень у березні 2021 року був опублікований доопрацьований проєкт закону, який зазнав значної критики через надані INCD повноваження та питання захисту приватності громадян [8].

Китай, навпаки, базує свою модель на концепції «кіберсуверенітету». Це означає, що держава володіє повним контролем над інформаційним середовищем у межах своїх кордонів. Такий підхід передбачає фільтрацію контенту, блокування доступу до окремих ресурсів, регулювання цифрових компаній та використання потужної системи моніторингу – «Золотого щита». Китайський досвід є прикладом централізованого управління цифровим простором як інструменту ідеологічного впливу та безпеки.

Отже, усі ці моделі мають свої сильні сторони – від технологічного лідерства до соціальної інклюзивності

та правової адаптивності. Спільним для них є те, що інформаційна безпека трактується як багатоаспектне явище, що охоплює законодавчий, технологічний, організаційний, освітній і міжнародний рівні. В умовах нових викликів особливої актуальності набуває міжнародна співпраця, що містить обмін кіберінформацією, розроблення єдиних стандартів та координацію реагування на інциденти.

Усі згадані моделі демонструють важливість комплексного, стратегічного та динамічного підходу до захисту національного інформаційного простору. Їх аналіз дозволяє виокремити позитивні елементи, які можуть бути адаптовані Україною:

1. Інституційна інтеграція: створення єдиного національного координаційного центру з питань інформаційної безпеки з міжвідомчим статусом (за прикладом США).

2. Гармонізація законодавства: приведення українських норм у відповідність до європейських стандартів (NIS2), що полегшить інтеграцію в єдиний цифровий ринок.

3. Цифрова освіта: масштабування програм цифрової грамотності, внесення тем інформаційної безпеки до навчальних курсів усіх рівнів освіти (за прикладом Естонії та ЄС).

4. Безпечне електронне урядування: впровадження єдиної цифрової ідентифікації громадян та захищених державних онлайн-сервісів.

5. Підготовка фахівців: створення кіберрезерву, підтримка ІТ-освіти та партнерств між державою, університетами і бізнесом (як в Ізраїлі).

6. Міжнародна кооперація: розширення участі в міжнародних кіберструктурах, обміні інформацією, спільних тренуваннях та стандартах.

7. Громадський контроль: забезпечення прозорості державної політики, інклюзивності процесів і залучення громадянського суспільства.

**Висновки.** Зарубіжний досвід переконливо свідчить, що ефективна система забезпечення національної безпеки в публічно-інформаційній сфері можлива лише за умови наявності чіткої стратегії, узгоджених дій між усіма суб’єктами безпеки, прозорої взаємодії з суспільством та постійного

вдосконалення відповідних механізмів. Україна має потенціал для адаптації найкращих практик – зокрема в напрямі розбудови кіберінфраструктури, посилення правового регулювання, підвищення цифрової грамотності та забезпечення стійкості інформаційного середовища до зовнішніх впливів. Необхідним є також розвиток системи підготовки кадрів у сфері інформаційної безпеки, створення міжвідомчих аналітичних центрів, а також активна участь у міжнародних ініціативах з кіберзахисту та протидії дезінформації.

## Список використаних джерел

1. Пугачов О. І. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* 2024. № 13. URL: https://reicst.com.ua/pmtl/article/view/2024-13-02-07/2024-13-02-07 (дата звернення: 20.05.2025).

2. Network and information security: proposal for a european policy approach (2014). URL: https://www.steptoe.com/a/web/485/811.pdf (дата звернення: 20.05.2025).

3. Act on the Federal Office for Information Security (BSI Act-BSIG). URL: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/BSI-Gesetz/bsi-gesetz.html (дата звернення: 20.05.2025).

4. Шемчук В. В. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Порівняльно-аналітичне право.* 2019. № 2. С. 188–191.

5. Климчук О. О., Ткачук Н. А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства, держави*. 2015. № 3. С. 75–83. URL: http://nbuv.gov.ua/UJRN/iblsd_2015_3_12 (дата звернення: 20.05.2025).

6. Дзеньків В. Кібербезпека в умовах сучасних загроз: ізраїльський досвід і його застосування в Україні. *Науковий вісник Ужгородського національного університету. Серія ПРАВО.* 2024. Вип. 84. Ч. 3. С. 77–83.

7. Гребенюк М. В., Леонов Б. Д. Досвід Ізраїлю у сфері забезпечення кібербезпеки. *Інформація і право.* 2018. № 2 (25). С. 45–50.

8. Stancu A.-I., Pavel T. Unveiling Israel's Cyber Legal Landscape: A Comprehensive Analysis of Cybersecurity Regulations and Policies. *Perspectives of Law and Public Administration.* 2023. № 12 (4). P. 643–650.

**Krushenitskyi V.,**
PhD student of the Department of Law and Law Enforcement Activity,
Volodymyr Vynnychenko Central Ukrainian State University,
Kropyvnytskyi, Ukraine
ORCID: 0000-0001-9194-7897

# FOREIGN EXPERIENCE IN ENSURING NATIONAL SECURITY IN THE PUBLIC INFORMATION SPHERE

*The article provides a comprehensive analysis of international models of ensuring information security in the context of globalization, digital transformation, and the growth of hybrid threats. The article reveals the strategic approaches of the world's leading states – the United States of America, the European Union, France, Germany, Israel, Poland, Estonia, and China – to the formation and implementation of information security policies. Attention is focused on institutional mechanisms, legal regulation, investment support, technological development, strategic communications systems, and digital literacy.*

*Particular attention was paid to the Israeli model, which combines a proactive approach to cyber defense, integration of scientific, military and business structures, development of an innovation ecosystem and functioning of a national regulator – INCD. In particular, the high level of investment, legislative initiative in the field of cybersecurity and the transformation of Israel into a global technological leader were noted.*

*The article also examines the EU's experience in harmonizing cybersecurity standards and digital education, the French concept of integrated security, the German legal approach to the protection of critical infrastructure, Estonia's model of the digital state, and China's system of total information space control based on the principles of "cyber sovereignty."*

*Based on the conducted analysis, the article proposes ways to improve Ukraine's information security system. In particular, it highlights the need to establish a unified national coordination body, harmonize legislation with European standards, implement digital education, expand international cooperation, and ensure public oversight.*

*The article emphasizes the importance of a strategic, systemic, and inclusive approach to information security as a key component of state policy and international resilience, with a focus on the effective adaptation of best global practices to the Ukrainian context.*

***Key words:*** *information security, cybersecurity, national security, security strategy, digital transformation, cyber infrastructure, critical infrastructure, cyber defense, disinformation, digital literacy, international cooperation, legal regulation, strategic communications.*

## References

1. Puhachov, O. I. (2024), "Foreign experience in ensuring state information security", *Problems of modern transformations. Series: law, public management and administration,* № 13, available at: https://reicst.com.ua/pmtl/article/view/2024-13-02-07/2024-13-02-07 (accessed 20 May 2025).

2. Network and information security: proposal for a european policy approach (2014), available at: https://www.steptoe.com/a/web/485/811.pdf (accessed 20 May 2025).

3. Act on the Federal Office for Information Security (BSI Act-BSIG), available at: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/BSI-Gesetz/bsi-gesetz.html (accessed 20 May 2025).

4. Shemchuk, V. V. (2019), "Foreign experience in ensuring state information security", *Comparative and analytical law,* № 2, pp. 188–191.

5. Klymchuk, O. O., Tkachuk, N. A. (2015), "The role and place of special services and law enforcement agencies of the worlds leading countries in national cybersecurity systems", *Information security of the person, society and state,* № 3, pp. 75–83, available at: http://nbuv.gov.ua/UJRN/iblsd_2015_3_12 (accessed 20 May 2025).

6. Dzenkiv, V. (2024), "Cybersecurity in the face of modern threats: Israeli experience and its application in Ukraine", *The collection of «Uzhhorod National University Herald. Series: Law»,* Vol. 84, part 3, pp. 77–83.

7. Hrebeniuk, M. V., Leonov, B. D. (2018), "Israels experience in cybersecurity", *Information and law,* № 2 (25), pp. 45–50.

8. Stancu, A.-I., Pavel, T. (2023), "Unveiling Israels Cyber Legal Landscape: A Comprehensive Analysis of Cybersecurity Regulations and Policies", *Perspectives of Law and Public Administration,* № 12 (4), pp. 643–650.